Reconnaissance faciale et libertés fondamentales : où en sommes-nous ?

Interview de Guillaume Desgens-Pasanau, magistrat et professeur associé au Cnam

Publié le 27 février 2020 – Mis à jour le 25 mars 2022

Des portiques de sécurité biométriques à l'entrée des établissements scolaires à la gourmandise en datas des GAFAMs, les projets et expérimentations de dispositifs utilisant la reconnaissance faciale rassurent autant qu'ils inquiètent, au point d'avoir amené la Cnil à publier en novembre dernier une série de recommandations appelant à un usage raisonné de cette technologie. En toile de fond de ces débats, un tiraillement entre enjeux sécuritaires et protection des libertés fondamentales semble inéluctable : la sécurité commence-t-elle nécessairement par-delà les frontières des libertés individuelles ? Quelles menaces réelles la reconnaissance faciale fait-elle aujourd'hui peser sur nos droits fondamentaux ? Guillaume Desgens-Pasanau, magistrat et professeur associé au Cnam spécialisé en droit du numérique, ancien directeur juridique de la Cnil, fait le point sur la législation existante… et sur ses limites.

© gece33 / IStock.com

Entre le déverrouillage d’un téléphone par reconnaissance faciale, qui fait déjà partie du quotidien de nombreux consommateurs, et l’identification des élèves à l’entrée d’un établissement scolaire, on a l’impression d’un changement d’échelle. Quelles limites à quelles utilisations de la reconnaissance faciale le RGPD pose-t-il aujourd’hui en France ?

La reconnaissance faciale n’est pas définie en tant que telle juridiquement. Du point de vue du Règlement général sur la protection des données (RGPD) et de la Cnil, la reconnaissance faciale est considérée comme **une donnée biométrique**, c’est-à-dire une donnée issue du corps humain, puisque c’est en fait l’analyse de la morphologie du visage qui va permettre d’identifier une personne et créer par exemple des accès, de la même manière qu’une empreinte digitale. Depuis l’adoption du RGPD, ce type de données a été ajouté à la liste des **données dites sensibles** , telles que celles sur la race, l’orientation sexuelle ou la santé… dont **la collecte est interdite**. La nouvelle règlementation ne dresse pas une liste des technologies plus intrusives que d’autres. Elle donne de grands principes et des exceptions, et notamment l’accord express de la personne concernée, ce que l’on appelle le **consentement**. Elle pose également un autre grand principe qui est celui de la **proportionnalité**, que la Cnil a par exemple fait valoir dans le cas de l’expérimentation dans un lycée à Nice d’un portique équipé d’un dispositif de reconnaissance faciale, au motif que **le contrôle des élèves à l’entrée d’un établissement pouvait être réalisé avec des technologies moins intrusives.** Là où le système est bien fait, c’est que consentement et proportionnalité se recoupent mais sont dissociables : **il ne suffit pas qu’un individu donne son consentement**pour qu’un tel dispositif soit mis en œuvre, s’il est par ailleurs manifestement disproportionné. L’analyse de proportionnalité est réalisée **au cas par cas**par la Cnil ou par le juge, par exemple en fonction du public visé. **Plus le public concerné est « vulnérable », comme des mineurs ou des salariés, plus l’analyse du principe de proportionnalité sera stricte. Il y a aussi plusieurs niveaux d’usages, mais plutôt en termes d’acteurs, selon qu’il s’agit qu’une entreprise privée ou d’une structure publique.**

Dans un contexte où les consommateurs et citoyens sont habitués à troquer leurs données personnelles contre l’accès à un service en ligne, pourquoi appeler le grand public à une vigilance toute particulière quant au développement des technologies de reconnaissance faciale ?

Là où la reconnaissance faciale franchit une étape supplémentaire par rapport aux autres types de données que nous fournissons habituellement, c’est qu’il s’agit d’**une donnée sensible, qui présente des risques spécifiques**. L’article 9 du RGPD liste une dizaine de données sensibles, dont il considère que leur collecte comporte aujourd’hui des risques pour les personnes concernées et qu’il faut « sanctuariser » au niveau européen. Les données biométriques en font partie, car comme les autres, elles représentent un risque important de **stigmatisation des personnes**selon les conditions dans lesquelles ces informations vont être utilisées. Le risque est notamment celui d’un **détournement de finalité**. La collecte en toute bonne foi des données biométriques par une entreprise ou une administration qui en a un besoin ne pose aucune difficulté ni au niveau du consentement ni au niveau de la proportionnalité. En revanche, **le problème posé est celui du stockage et de la réutilisation** de ces données pour d’autres finalités, comme lorsque des images de dispositifs de vidéo protection installés pour prévenir les infractions routières sont réutilisées pour l’instruction d’infractions qui n’ont rien à voir avec la sécurité routière. Le problème des données biométriques, c’est aussi qu’**elles ne sont pas encore suffisamment fiables sur le plan technique**, ce qui pose **un problème d’intégrité** selon la technologie utilisée, dans la mesure où on ne peut aujourd’hui pas toujours s’assurer que les données collectées sont exactes et pertinentes et identifient avec certitude la personne concernée. Le risque est donc celui d’une **usurpation d’identité**, dans le cas par exemple où une personne serait identifiée à tort comme étant l’auteur d’une infraction.

Depuis l'adoption du RGPD, la Cnil est-elle à même de jouer son rôle de garde-fou face aux velléités des GAFAMs, Facebook en tête, dont les expérimentations en matière de reconnaissance faciale agitent régulièrement le débat public ?

Par définition, les GAFAMs, ou plus largement les sites de commerce électronique, se financent largement avec nos données personnelles. Ceci étant dit, **il y a quand même des règles pour nous protéger**qui me semblent plutôt adaptées. Depuis le RGPD, la Cnil a une double fonction : elle a à la fois une fonction de conseil, mais aussi **de vrais pouvoirs de contrôle et de sanction**, ce qui est assez nouveau. Par exemple, en 2018, la Cnil a prononcé **une amende de 50 millions d'euros à l'encontre de Google**. En revanche, ces règles ne sont pas là pour nous protéger contre nous-mêmes. C'est là où se pose l'enjeu de **l'éducation au numérique**, notamment par rapport au consentement : l'acceptabilité des nouvelles technologies est de plus en plus forte chez les gens, notamment si elles avancent l'argument de la sécurité. **Il faut apprendre aux gens à ne pas dire oui tout le temps**et les informer sur les alternatives existantes.

C'est donc moins des expérimentations de Facebook que de celles de l'État dont il faut craindre qu'elles empiètent sur nos libertés ?

Avec le RGPD, le droit européen a fixé un cadre général de règles pour le secteur privé et pour les fichiers courants dans les administrations. Mais **pour tout ce qui touche à la sûreté de l'État, à la sécurité publique, à la justice, à la police, à la défense, il y a ce que l'on appelle une directive européenne, qui laisse beaucoup plus de marge de manœuvre aux États.** Le droit français peut donc créer **des textes dérogatoires**, qui permettent par exemple actuellement d'installer de plus en plus de caméras de vidéosurveillance au motif de lutter contre la violence routière. **En dématérialisant le contrôle routier à Paris, le nombre de ces caméras s'est multiplié par 5 ou 6**, ce qui va dans le sens du grignotage de nos libertés : **parmi les droits fondamentaux garantis constitutionnellement, il y a la liberté de circuler, c'est-à-dire de se déplacer librement, anonymement, sans être surveillé**. Quant au **droit à l'oubli**, il implique que les images des caméras de vidéosurveillance soient supprimées automatiquement tous les 30 jours, mais **il arrive que des contrôles de la Cnil mettent en évidence des données conservées plus longtemps que prévu.** Entre mettre en place des dispositifs qui vont renforcer la sécurité des gens sans pour autant grignoter la vie privée, le problème est de savoir où l'on fixe la limite. **En ce moment, la limite se déplace très significativement au niveau des enjeux de sécurité.**Pour l'instant, les règles concernant la reconnaissance faciale sont plutôt sévères, mais le risque est que demain, par le biais de réformes législatives, elles viennent à s'assouplir comme c'est le cas actuellement sur la vidéosurveillance. Sachant qu'une fois une mesure dérogatoire adoptée,**l'effet de « cliquet »** fait que l'on ne revient jamais en arrière.

Le projet d'application mobile Alicem, visant à utiliser la reconnaissance faciale pour authentifier l'utilisateur au moment de la création d'un compte unique pour accéder aux services en ligne de plusieurs administrations publiques, représente-t-il selon vous une menace potentielle pour les libertés individuelles ?

Il faut savoir que les règles de protection des données en France existent depuis plus de 40 ans et ont été créées pour **protéger les individus contre le fichage par l'État**, notamment quand on a commencé à utiliser le numéro de sécurité sociale, qui est un identifiant unique très fort. À l'époque, il a été question de faire **des interconnexions entre les différents fichiers** : ceux de la police, ceux du Trésor Public, pour permettre de tout savoir sur une seule personne. **La loi Informatique et libertés, adoptée en 1978**, a justement été adoptée pour signaler qu'interconnecter toutes les informations sur la base d'un identifiant unique était la limite à ne pas franchir et qu'il fallait continuer de cloisonner l'information. **Le problème des nouvelles technologies, c'est justement qu'elles peuvent permettre de faire ces interconnexions.**Le projet Alicem est un peu différent, car il vise juste à utiliser un identifiant unique sans pour autant que les bases de données soient interconnectées, mais **il faut rester vigilent concernant tout usage éventuellement disproportionné de cette technologie**, car cela pourrait être un pas vers la création d'un méga fichier.

Propos recueillis par Laetitia Casas,

Journaliste à Direction de la Communication

| Citoyenneté | Droit | Innovation | Numérique | Sécurité | Société

Vous souhaitez vous former en droit du numérique et au RGPD ?

Découvrez l'offre de formation du Cnam !

UE "Droit des technologies de l'information et de la communication"

UE "Métier du délégué à la protection des données"

UE "Droit des nouvelles technologies, de l'information et de la communication : perfectionnement"

Certificat de spécialisation "Délégué à la protection des données (DPO/CIL)"

L'auteur

Guillaume Desgens-Pasanau, magistrat, professeur associé et responsable national du certificat de spécialisation Délégué à la protection des données.
Découvrez son blog consacré à l'actualité en matière de protection des données.

+ tous ses articles